CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

March 10, 2006

S. 1326
Notification of Risk to Personal Data Act

As reported by the Senate Committee on the Judiciary on October 20, 2005

SUMMARY

S. 1326 would require all government and private-sector entities in possession of sensitive personal information to implement and maintain reasonable security procedures and practices to prevent unauthorized disclosure of such information. In the event of a security breach that creates a significant risk of identity theft, those entities would be required to notify all individuals whose personal information was compromised. The legislation defines sensitive personal information as combinations of an individual's name, address or phone number, and Social Security number, driver's license number, or financial account information. S. 1326 also would create civil penalties for entities that fail to provide notice of security breaches to affected individuals.

Complying with the bill's provisions would increase the administrative expenses of federal agencies. CBO estimates that those added costs would sum to about $10 million over the 2006-2011 period and would generally come from agencies' salary and expenses budgets, which are subject to annual appropriation. Implementing S. 1326 could increase collections of civil penalties, which would affect direct spending and revenues, but CBO estimates that such effects would not be significant in any year.

S. 1326 contains several intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), including requirements to secure databases containing sensitive personal information, potentially costly notification requirements, and explicit preemptions of the authority of State Attorneys General and state law. While the aggregate cost of complying with these mandates is uncertain, CBO estimates that the costs to state, local, and tribal governments would likely exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years after the mandates go into effect.

S. 1326 also would impose private-sector mandates on certain private-sector entities, including partnerships, individuals, corporations, and associations that own or license

computerized data containing sensitive personal information. While CBO cannot estimate the direct cost of complying with each mandate, the bill would impose security and notification procedures and practices on a large number of private-sector entities, including more than five million employers. Based on this information, CBO estimates that the total direct cost of the mandates would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of S. 1326 is shown in the following table. The costs of the legislation fall primarily in function 370 (commerce and housing credit).

	By Fiscal Year, In Millions of Dollars					
	2006	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION[a]						
Estimated Authorization Level	1	2	2	2	2	2
Estimated Outlays	1	2	2	2	2	2

a. Enacting S.1326 also could affect direct spending and revenues, but CBO estimates that any such effects would not be significant.

BASIS OF ESTIMATE

CBO estimates that implementing S. 1326 would cost about $10 million over the 2006-2011 period, assuming the appropriation of the necessary amounts. Enacting the bill could increase both direct spending and receipts, but CBO expects that any such effects would not be significant in any year.

Spending Subject to Appropriation

The Federal Information Security Management Act of 2002 provides requirements for securing the federal government's information systems, including protecting personal privacy. The National Institute of Standards and Technology develops information security standards and guidelines for other federal agencies, and the Office of Management and Budget (OMB) oversees security policies and practices for information technology. OMB

estimates that federal agencies spend around $5 billion a year to secure the government's computer information systems.

In the event of a security breach involving a significant risk of identity theft, government agencies would be required to notify an individual whose information may have been compromised. However, S. 1326 would cap the costs at $250,000 per incident. CBO cannot estimate the number of security breaches with a significant risk of identity theft that would occur in any one year. While it is uncertain how often these breaches will occur, using information from OMB and other agencies, CBO does not expect that government agencies would incur significant notification costs in any one year. Thus, CBO estimates that implementing S. 1326 would not significantly increase the costs of ongoing efforts to maintain secure federal computer systems and deter identity theft.

Subject to the availability of appropriated funds, CBO estimates that implementing S. 1326 would cost about $10 million over the 2006-2011 period for federal agencies to enforce compliance with the legislation by state and local governments and private-sector entities and assess fines related to identity theft.

Direct Spending and Receipts

CBO estimates that enacting S. 1326 would increase direct spending by less than $500,000 annually. In addition, CBO estimates that the new civil penalties imposed by the legislation would result in an increase in revenues of less than $500,000 annually.

Regulatory Agencies. S. 1326 would direct many government entities, including the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), Federal Deposit Insurance Corporation (FDIC), Farm Credit Administration, and the Board of Governors of the Federal Reserve System, to enforce compliance and assess fines as they apply to financial institutions. The OCC, OTS, NCUA, and Farm Credit Administration assess fees to pay for their administrative costs; therefore, any additional spending by those agencies to implement the bill would have no net budgetary effect. The FDIC, however, uses insurance premiums paid by all banks to cover the expenses it incurs to supervise state-chartered banks. The bill's requirements for the FDIC would cause a small increase in spending, but would not affect its premium income. In total, CBO estimates that S. 1326 would increase net direct spending of the OCC, NCUA, OTS, Farm Credit Administration, and FDIC by less than $500,000 a year.

Budgetary effects on the Federal Reserve are recorded as changes in revenues (governmental receipts). The Federal Reserve earns interest on its holdings of government securities and

subtracts its operating costs before remitting the rest to the Treasury as revenue. CBO estimates that enacting S. 1326 would not result in significant costs.

Civil Penalties. S. 1326 would establish new federal crimes for the failure to notify individual(s) that their personal information was compromised through unauthorized access. Enacting the bill could increase collections of civil fines for violations of the bill's provisions. CBO estimates that any additional collections would not be significant because of the relatively small number of additional cases likely to be affected. Civil fines are recorded in the budget as revenues and deposited in the Treasury.

IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 1326 contains several intergovernmental mandates as defined in UMRA. Specifically, the bill would:

- Require that state and local governments—including public schools and universities—implement and maintain certain security procedures;

- Require that state and local governments—including public schools and universities—notify affected individuals and credit-reporting agencies of any breach of security that could result in identity theft;

- Explicitly preempt state laws regarding the treatment of personal information in at least 19 states; and

- Place certain notification requirements and limitations on state attorneys general and state insurance authorities.

While the aggregate costs of complying with the mandates is uncertain, CBO estimates that the notification requirements and the requirements to implement and maintain certain security procedures would impose the most significant costs on state and local governments. The remainder of this analysis focuses on those requirements. CBO estimates that the costs of these provisions to state, local, and tribal governments would likely exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation) in at least one of the first five years that the mandates go into effect.

Notification Requirements

In the event of a security breach meeting certain conditions, the bill would require state and local governments to notify any individual whose information may have been compromised, provide a toll-free number or Web site that affected individuals can use for further information, and coordinate with consumer reporting agencies. The bill would cap costs for each notification at $250,000, but examples from California suggest that a large university could expect to incur costs of between $100,000 and $200,000 to notify individuals whose personal information may have been compromised.

Entities that would be affected by those requirements include, but are not limited to, state departments of revenue and motor vehicles, public hospitals, courts at the state and local levels, agencies that oversee elections, K-12 schools, school districts, and post-secondary institutions. There are more than 190,000 such entities in the United States (75,000 municipal governments, about 3,600 counties, more than 100 public hospitals, about 100,000 schools, 14,000 school districts, and more than 1,500 public post-secondary institutions). Relatively few of these entities would have to experience a security breach for costs to be significant in any one year. For example, if the average cost to comply with the notification mandate was $50,000, less than 1 percent of intergovernmental entities that maintain databases would need to suffer a security breach for the threshold established in UMRA to be exceeded. According to data security experts, security breaches have been increasing substantially over time. While CBO cannot estimate the frequency or targets of such breaches, we expect that the costs would be significant and would likely grow over time.

Reasonable Security Requirements

The bill would require any state or local government that owns computerized data containing sensitive personal information to implement and maintain reasonable security procedures and practices. While the bill does not define reasonable security requirements, if state and local governments do not currently have a system in place to safeguard sensitive personal information, they would have to implement such a system. If they do have a system, they might have to upgrade their systems. Due to the large number of entities involved, even small, one-time costs—for example, as little as $1,000—would impose significant costs, in aggregate, on intergovernmental entities.

IMPACT ON THE PRIVATE SECTOR

S. 1326 would impose private-sector mandates on partnerships, individuals, corporations, and associations that own or license computerized data containing sensitive personal information. The act defines sensitive personal information as a combination of an individual's name, address or telephone number, and Social Security number, driver's license number, financial account number, or debit or credit card information. While CBO cannot estimate the direct cost of complying with each mandate, the bill would impose security and notification procedures and practices on a large number of private-sector entities, including more than five million employers. Based on this information, CBO estimates that the total direct cost of the mandates would exceed the annual threshold established by UMRA for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Security Requirements

S. 1326 would require covered entities to implement and maintain reasonable security procedures and practices to protect sensitive personal information from security breaches. Covered entities would include individuals, partnerships, corporations, associations, and private organizations that own or license computerized data containing sensitive personal information. Since the bill does not define what reasonable security procedures and practices are, CBO does not have enough information to estimate the average cost to an entity to comply with the mandate. Because of the large number of covered entities, however, we expect that even if the average cost of compliance was small, the overall costs of this mandate could be large relative to UMRA's threshold for private-sector mandates.

Notification of Security Breach

In the case of a security breach, the bill would require covered entities to investigate any suspected breach of security to determine whether a significant risk of identity theft exists. If the breach creates a reasonable risk of identity theft, the entity would be required to notify all those individuals whose personal information was compromised, to provide a toll-free telephone number or Web site that affected individuals can use for further information, and to notify all nationwide credit-reporting agencies if the breach affects 1,000 or more individuals. Notice may be provided in writing, by telephone, or by e-mail to affected individuals. If the compromised information is not owned or licensed by the entity investigating the breach, then the entity must notify the owner or licensor of the compromised information.

The cost of this mandate depends on the number of security breaches that occur, the average number of persons affected by a breach, and the cost per person of notification. There is very little information available on the number of breaches each year; only the largest of breaches are noticed and recorded. Nevertheless, what information is available suggests that security breaches are not rare. Although the cost to notify one person by mail might be about $2, the potentially large number of people in data systems maintained by some covered entities would make the cost of notification associated with one breach significant. CBO estimates that the costs imposed by the consumer notification requirement also could be large relative to UMRA's threshold for private-sector mandates.

PREVIOUS CBO ESTIMATE

On November 3, 2005, CBO transmitted a cost estimate for S. 1408, the Identity Theft Protection Act, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on July 28, 2005. The two pieces of legislation have similar provisions related to identity theft, but S. 1326 has broader authorities. The cost estimates reflect those differences. In addition, S. 1408 would impose private-sector mandates on certain private entities and consumer credit-reporting agencies that acquire, maintain, or utilize sensitive personal information Since the bill would impose security standards and notification requirements on a large number of private-sector entities, CBO estimated that the total direct cost of mandates in the bill would exceed the annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation). S. 1326 would impose similar notification requirements on most of the same private-sector entities.

ESTIMATE PREPARED BY:

Federal Costs: Matthew Pickford
Impact on State, Local, and Tribal Governments: Sarah Puro
Impact on the Private Sector: Patrice Gordon

ESTIMATE APPROVED BY:

Peter H. Fontaine
Deputy Assistant Director for Budget Analysis